FortiClient EMS for Chromebooks - QuickStart Guide

Version 1.2.3

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTIGATE COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING SERVICES
http://www.fortinet.com/training

FORTIGUARD CENTER
http://www.fortiguard.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

January 8, 2018
FortiClient EMS for Chromebooks 1.2.3 QuickStart Guide
04-123-408700-20180108

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-12-12	Initial release.
2018-01-08	Updated Supported installation platforms on page 6.

Introduction

This guide describes how to install and set up FortiClient Enterprise Management Server (EMS) for Chromebooks. It also describes how to set up the Google Admin console to use the FortiClient Web Filter extension. Together the products provide web filtering for Google Chromebook users.

Supported installation platforms

You can install FortiClient EMS for Chromebooks on the following platforms:

- Microsoft Windows Server 2008 R2 or newer

For information about minimum system requirements and supported platforms, see the *FortiClient EMS for Chromebooks Release Notes*, available in the Fortinet Document Library.

Requirements

The following components and knowledge are required to use FortiClient EMS for Chromebooks:

- FortiClient EMS for Chromebooks installer
- FortiClient Web Filter extension available in the Google Web Store for Chrome OS
- G Suite account
- Knowledge of administering the Google Admin console
- A domain configured in the Google Admin console
- SSL certificate to support communication between FortiClient Web Filter extension and FortiClient EMS for Chromebooks
- SSL certificate to support communication between FortiClient Web Filter extension and FortiAnalyzer for logging, if using
- Unique set of service account credentials

Required services and ports

You must ensure required ports and services are enabled for use by FortiClient EMS for Chromebooks and its associated applications on your server. The required ports and services enable FortiClient EMS for Chromebooks to communicate with endpoints and servers running associated applications.

Communication	Service	Protocol	Port
Apache	HTTPS	TCP	443
SQL server			
FortiClient on Chrome OS • Connection to Profile Server.			8443 (default) You can customize this port.

G Suite account

You need to sign up for your G Suite account before you can use the Google service and manage your Chromebook users.

The G Suite account is different from the free consumer account. The G Suite account is a paid account that gives access to a range of Google tools, services, and technology.

You can sign up for a G Suite account here: https://gsuite.google.com/signup/basic/welcome#0

In the sign up process, you must use your email address to verify your Google domain. This also proves you have ownership of the domain.

SSL certificates

FortiClient EMS for Chromebooks requires an SSL certificate signed by a Certificate Authority (CA) in pfx format. Use your CA to generate a certificate file in pfx format, and remember the configured password. For example, the certificate file name is *server.pfx* with password 111111.

The server where FortiClient EMS for Chromebooks is installed should have a fully qualified domain name (FQDN), such as ems.forticlient.com, and you must specify the FQDN in your SSL certificate.

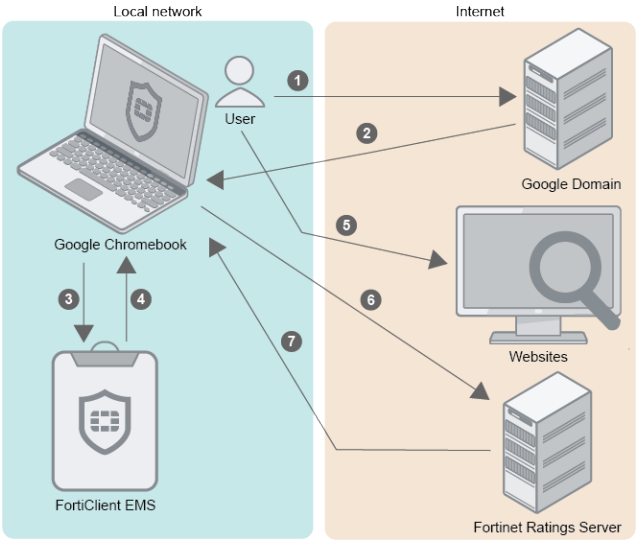
If you are using a public SSL certificate, the FQDN can be included in *Common Name* or *Subject Alternative Name*. You must add the SSL certificate to FortiClient EMS for Chromebooks. See Adding SSL certificates to FortiClient EMS for Chromebooks on page 27. You do not need to add the root certificate to the Google Admin console.

If you are using a self-signed certificate (non-public SSL certificate), your certificate's *Subject Alternative Name* must include `DNS:<FQDN>`, for example, `DNS:ems.forticlient.com`. You must add the SSL certificate to FortiClient EMS for Chromebooks and the root certificate to the Google Admin console to allow the extension to trust FortiClient EMS for Chromebooks. See Adding root certificates on page 15.

How the products work together

After you install and configure FortiClient EMS for Chromebooks, the Google Admin console, and the FortiClient Web Filter extension, the products work together to provide web filtering security for Google Chromebook users logged into the Google domain. Following is a summary of how the products work together after the setup is complete:

1. A user logs into the Google Chromebook.
2. The Google Chromebook downloads the FortiClient Web Filter extension.
3. FortiClient connects to FortiClient EMS for Chromebooks.
4. FortiClient downloads a profile to the Google Chromebook. The profile contains web filtering settings from FortiClient EMS for Chromebooks.
5. The user browses the Internet on the Google Chromebook.
6. FortiClient sends the URL query to the Fortinet Ratings Server.
7. The Fortinet Ratings Server returns the category result to FortiClient. FortiClient compares the category results with the profile to determine whether to allow the Google Chromebook user to access the URL.



Installation

Following is a summary of how to install and start FortiClient EMS for Chromebooks:

1. Download the installation file. See Downloading the installation file on page 9.
2. Install FortiClient EMS for Chromebooks. See Installing FortiClient EMS for Chromebooks on page 9.
3. Start FortiClient EMS for Chromebooks and log in. See Starting FortiClient EMS for Chromebooks and logging in on page 11.

Downloading the installation file

FortiClient EMS for Chromebooks is available for download from the following location:

Fortinet Support website: https://support.fortinet.com/

You can also receive the installation file from a sales representative.

The following installation file is available for FortiClient EMS for Chromebooks:

`FortiClientEnterpriseManagement_Chromebook_1.2.3.<build>_x64.exe`

For information about obtaining FortiClient EMS for Chromebooks, contact your Fortinet reseller.

Installing FortiClient EMS for Chromebooks

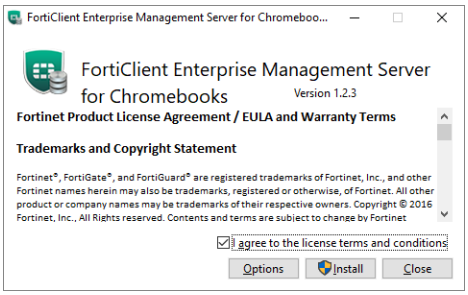
The FortiClient EMS for Chromebooks installation package includes:

- FortiClient EMS for Chromebooks
- Microsoft SQL Server 2014 Express Edition
- Apache HTTP server

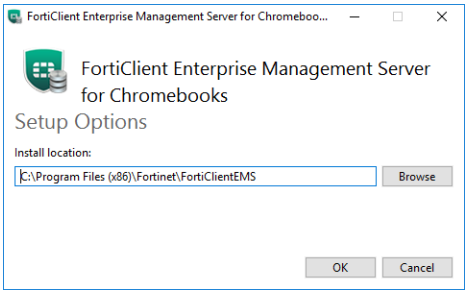
Local administrator rights and Internet access are required to install FortiClient EMS for Chromebooks.

To install FortiClient EMS for Chromebooks:

1. If you are logged into the system as an administrator, double-click the downloaded installation file.
   If you are not logged in as an administrator, right-click the installation file, and select *Run as administrator*.
2. If applicable, select *Yes* in the *User Account Control* window to allow the program to make changes to your system.
3. In the installation window, select *I agree to the license terms and conditions* if you agree with the license terms and conditions. If you do not agree, you cannot install the software.



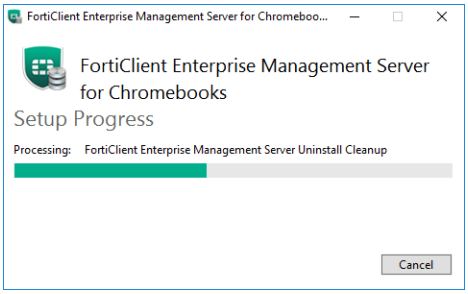
4. (Optional) Click *Options* to specify a custom directory for the FortiClient EMS for Chromebooks installation.



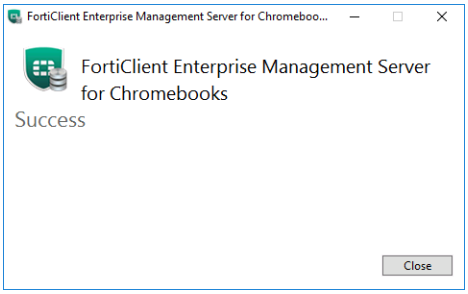
   a. Click *Browse* to locate and select the custom directory.
   b. Click *OK* to return to the installation wizard.

5. Click *Install*.

   The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others.



6. When the program has installed correctly, the *Success* window displays. Click *Close*.



   A *FortiClient Enterprise Management Server* icon is added to the desktop.

Extending license expiries

You can apply multiple licenses to your FortiClient EMS for Chromebooks to extend the license expiry. For example, consider you purchase two one-year licenses for FortiClient EMS for Chromebooks. After you register and apply the first license, FortiClient EMS for Chromebooks has an expiry date of August 1, 2018. You can register and apply the second license as a renewal, after which FortiClient EMS for Chromebooks has an expiry date of August 1, 2019.

Note you must upload the second license file to FortiClient EMS for Chromebooks using the GUI. Registering the license does not automatically update the license expiry in FortiClient EMS for Chromebooks.

Using a second license to extend the license expiry date does not increase the number of licensed clients. To increase the number of licensed clients, contact Fortinet Support for a co-term contract.

For details, see the *FortiClient EMS for Chromebooks Administration Guide*.

Starting FortiClient EMS for Chromebooks and logging in

FortiClient EMS for Chromebooks runs as a service on Windows computers.

To start FortiClient EMS for Chromebooks:

1. Double-click the *FortiClient Enterprise Management Server for Chromebooks* icon.
2. Sign in with the username *admin* and no password.
3. Change the username and password by going to *Administration* > *Administrators*.
4. Configure FortiClient EMS for Chromebooks by going to *System Settings*.

Accessing FortiClient EMS for Chromebooks remotely

You can access FortiClient EMS for Chromebooks remotely using a web browser instead of the GUI.

To enable remote access to FortiClient EMS for Chromebooks:

1. Go to *System Settings* > *Server*.
2. Enable *Remote HTTPS access*.
3. If desired, in the *Custom hostname* box, type the host name or IP address. Otherwise, the *Pre-defined hostname* is used.
4. If desired, select the *Redirect HTTP request to HTTPS* checkbox. If this option is enabled, if you attempt to remotely access EMS at *http://<server_name>*, this is automatically redirected to *https://<server_name>*.
5. Click *Save*.

To remotely access FortiClient EMS for Chromebooks:

- To access EMS from the EMS server, visit `https://localhost`
- To access the server remotely, use the server's hostname: `https://<server_name>`
  Ensure you can ping `<server_name>` remotely. This can be achieved by adding it into a DNS entry or to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

Google Admin Console Setup

This section describes how to add and configure the FortiClient Web Filter extension on Chromebooks enrolled in the Google domain.

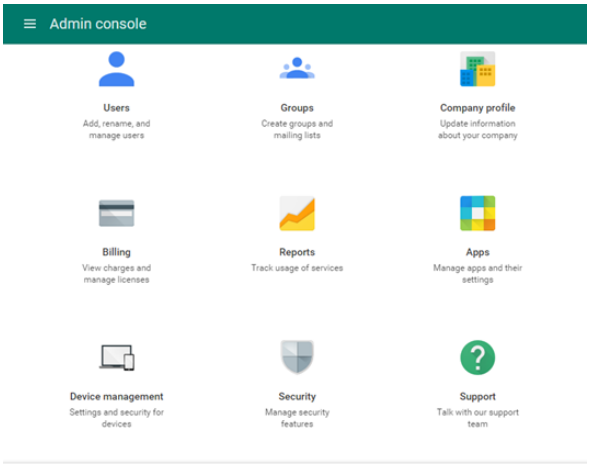
Following is a summary of how to set up the Google Admin console:

1. Log into the Google Admin console. See Logging into the Google Admin console on page 13.
2. Add the FortiClient Web Filter extension. See Adding the FortiClient Web Filter extension on page 13.
3. Configure the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 14.
4. Add the root certificate. See Adding root certificates on page 15.

Logging into the Google Admin console

To log into the Google Admin console:

1. Log into the Google Admin console (https://admin.google.com) using your Google domain admin account. The Admin console displays.

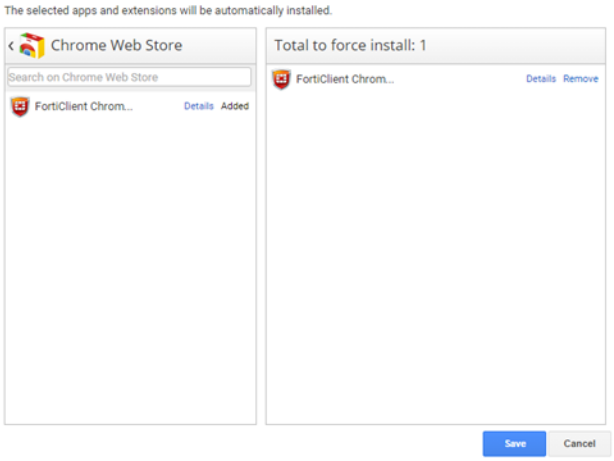


Adding the FortiClient Web Filter extension

FortiClient EMS for Chromebooks software is not available for public use. You can only enable the feature using the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao

To add the FortiClient Web Filter extension:

1. In the Google Admin console, go to *Device management* > *Chrome Management* > *User Settings* > *Apps and Extensions* > *Force-installed Apps and Extensions* > *Manage force-installed apps*.
2. Select *Chrome Web Store*, and search for the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao.
3. Add the extension ID and save.
   The extension name displays as *FortiClient Chromebook Web Filter Extension*.



Configuring the FortiClient Web Filter extension

You must configure the FortiClient Chromebook Web Filter extension to enable the Google Admin console to communicate with FortiClient EMS for Chromebooks.

FortiClient EMS for Chromebooks hosts the services that assign endpoint profiles of web filtering policies to groups in the Google domain. FortiClient EMS for Chromebooks also handles the logs and web access statistics sent from the FortiClient Web Filter extensions.

FortiClient EMS for Chromebooks is the profile server.

To configure the FortiClient Web Filter extension:

1. In FortiClient EMS for Chromebooks, locate the server name and port by going to *System Settings* > *EMS for Chromebooks*.
2. Create a text file that contains the following text:

```
{
   "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >"}
}
```

   For example:

```
{
   "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443”}
}
```

3. In the Google Admin console, go to *Device management* > *Chrome Management* > *App Management* > *FortiClient Chrome Web Filter Extension* > *User settings*.
4. Click a domain or organization unit (OU).
5. In the right pane, under *Configure*, upload a new configuration file.

   You can also view the current settings.
6. Click *Save*.
7. Go to *Device Management* > *Chrome* > *App Management* to view your configured Chrome apps.

Adding root certificates

This section includes the following information:

Communication with the FortiClient Chromebook Web Filter extension

The FortiClient Chromebook Web Filter extension communicates with FortiClient EMS for Chromebooks using HTTPS connections. The HTTPS connections require an SSL certificate. You must obtain an SSL certificate and add it to FortiClient EMS for Chromebooks to allow the extension to trust FortiClient EMS for Chromebooks.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiClient EMS for Chromebooks. See Adding SSL certificates to FortiClient EMS for Chromebooks on page 27.

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiClient EMS for Chromebooks and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS for Chromebooks will not work. See Uploading root certificates to the Google Admin console on page 17.

Communication with FortiAnalyzer for logging

This section applies only if you are sending logs from FortiClient EMS for Chromebooks to FortiAnalyzer. If you are not sending logs, skip this section.

Sending logs to FortiAnalyzer requires you enable ADOMs in FortiAnalyzer and add FortiClient EMS for Chromebooks to FortiAnalyzer. FortiClient EMS for Chromebooks is added as a device to the FortiClient ADOM in FortiAnalyzer. See the *FortiAnalyzer Administration Guide*.

FortiClient EMS for Chromebooks supports logging to FortiAnalyzer. If you have a FortiAnalyzer device and configure FortiClient EMS for Chromebooks to send logs to FortiAnalyzer, a FortiAnalyzer CLI command must be enabled and an SSL certificate is required to support communication between the FortiClient Web Filter extension and FortiAnalyzer.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiAnalyzer. See Adding SSL certificates to FortiAnalyzer.

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiAnalyzer and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiAnalyzer will not work. See Uploading root certificates to the Google Admin console on page 17.

The FortiAnalyzer IP address should be specified in the SSL certificate. If you are using a public SSL certificate, the FortiAnalyzer IP address can be assigned to *Common Name* or *Alternative Name*. If you are using a self-signed (nonpublic) SSL certificate, your certificate's *Subject Alternative Name* must include `IP:<FortiAnalyzer IP>`.

Enabling HTTP and HTTPS logging access to FortiAnalyzer

You must use the FortiAnalyzer CLI to add HTTP-logging and HTTPS-logging to the allow-access list in FortiAnalyzer. This command is one step in the process that allows FortiAnalyzer to receive logs from FortiClient EMS for Chromebooks.

In FortiAnalyzer CLI, enter the following command:

```
config system interface
   edit "port1"
      set allowaccess https ssh http http-logging https-logging
   next
end
```

Adding SSL certificates to FortiAnalyzer

To add SSL certificates to FortiAnalyzer:

1. In FortiAnalyzer, go to *System Settings* > *Certificates* > *Local Certificates*.
2. Click *Import*. The *Import Local Certificate* dialog appears.
3. In the *Type* list, select *Certificate* or *PKCS #12 Certificate*.
4. Beside *Certificate File*, click *Browse* to select the certificate.
5. Enter the password and certificate name.
6. Click *OK*.

Summary of where to add certificates

The following table summarizes where to add certificates to support communication with the FortiClient Web Filter extension and FortiAnalyzer.

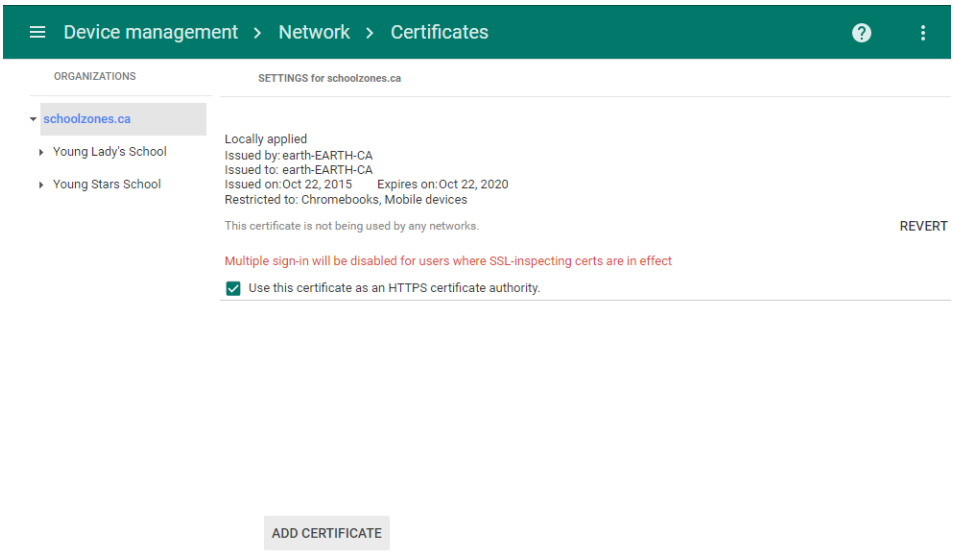
Scenario	Certificate and CA	Where to Add Certificates
Allow the FortiClient Chromebook Web Filter extension to trust EMS	Public SSL certificate	• Add SSL certificate to FortiClient EMS for Chromebooks.
	SSL certificate not from a common CA	• Add SSL certificate to FortiClient EMS for Chromebooks. • Add your certificate's root CA to the Google Admin console.
Allow the FortiClient Chromebook Web Filter extension to trust FortiAnalyzer for logging	Public SSL certificate	• Add SSL certificate to FortiAnalyzer.
	SSL certificate not from a common CA	• Add SSL certificate to FortiAnalyzer. • Add your certificate's root CA to the Google Admin console.

Uploading root certificates to the Google Admin console

To add root certificates:

1. In the Google Admin console, go to *Device Management* > *Network* > *Certificates (root certificate) (crt certificate)*.
2. Add the root certificate.
3. Select the *Use this certificate as an HTTPS certificate authority* checkbox.

Do not forget to select the *Use this certificate as an HTTPS certificate authority* checkbox.



Disabling access to Chrome developer tools

It is recommended to disable access to Chrome developer tools. This blocks users from disabling the FortiClient Web Filter extension.

To disable access to Chrome developer tools:

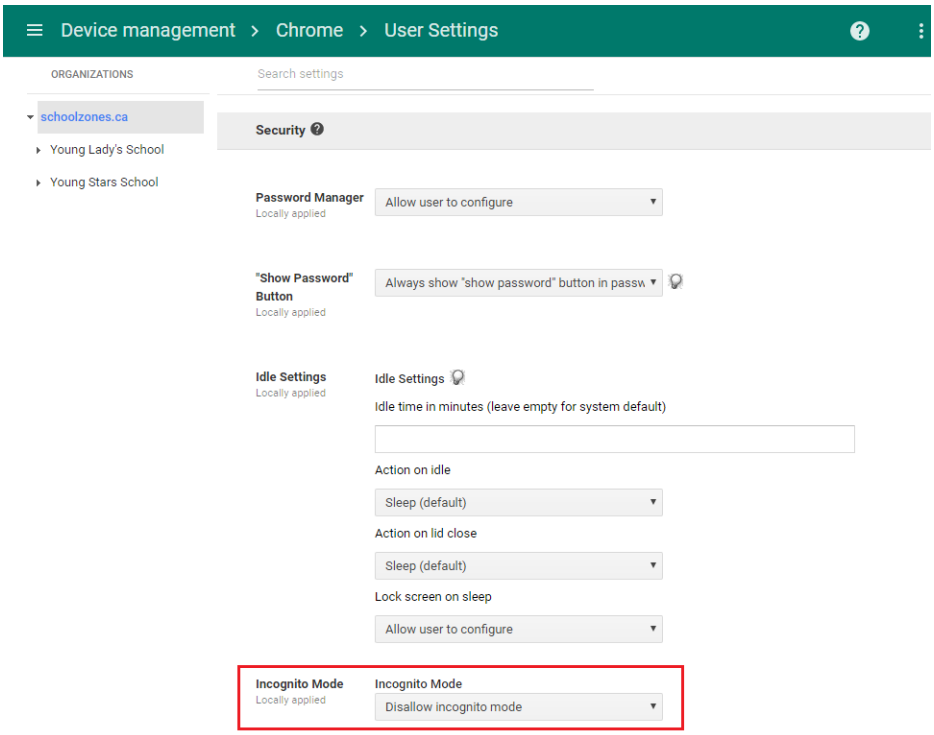
1. In the Google Admin console, go to *Device management* > *Chrome Management* > *User Settings*.
2. For the *Developer Tools* option, select *Never allow use of built-in developer tools*.

Disallowing incognito mode

When users browse in incognito mode, extensions are bypassed. Incognito mode should be disallowed for managed Google domains.

To disallow incognito mode:

1. In the Google Admin console, go to *Device management* > *Chrome management* > *User settings*.
2. From the left panel, select the organization.
3. In the *Security* section, set *Incognito Mode* to *Disallow incognito mode*.



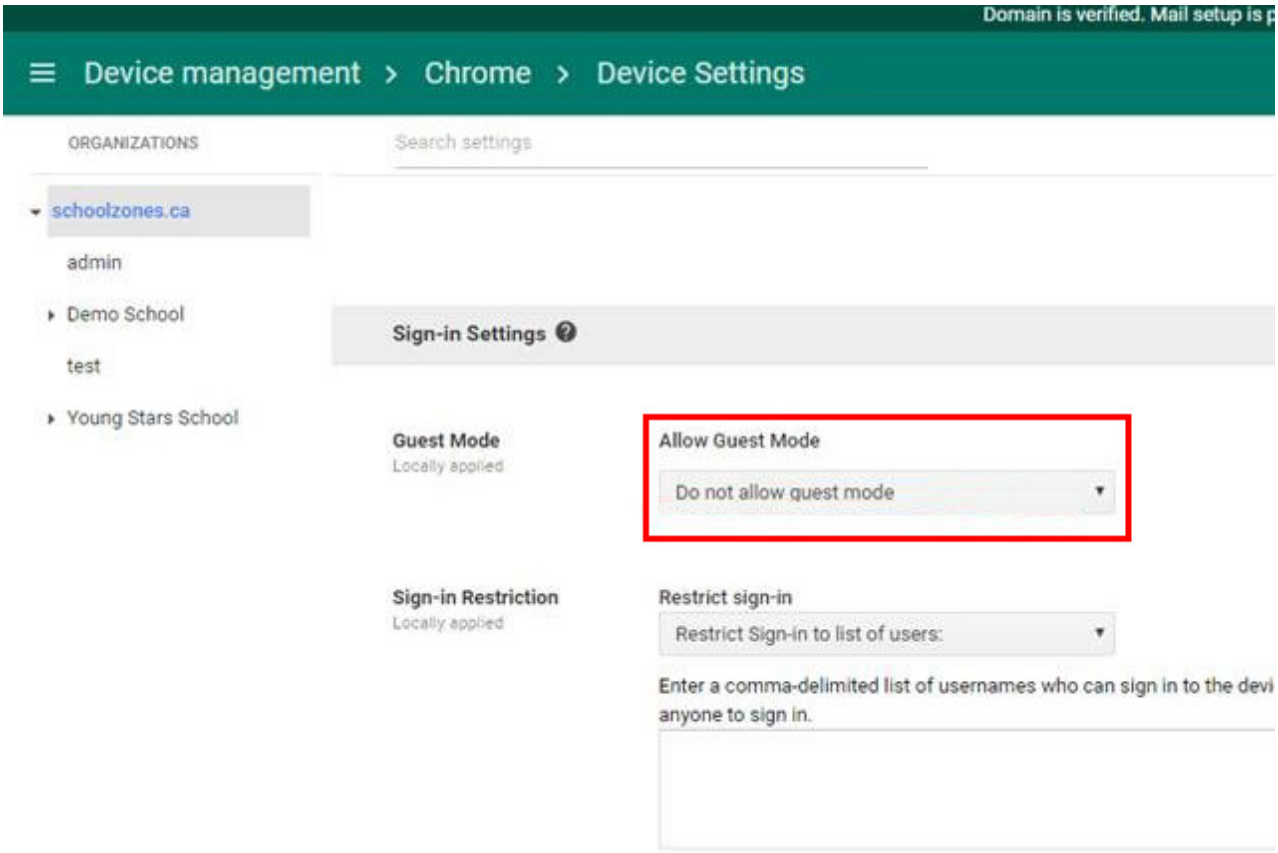
4. Click *Save*.

Disallowing guest mode

Guest mode should be disallowed for managed Google domains.

To disallow guest mode:

1. In the Google Admin console, go to *Device management* > *Chrome management* > *Device settings* > *Sign-in settings*.
2. From the left panel, select the organization.
3. Under *Guest Mode*, select *Do not allow guest mode* from the *Allow Guest Mode* dropdown list.



4. Click *Save*.

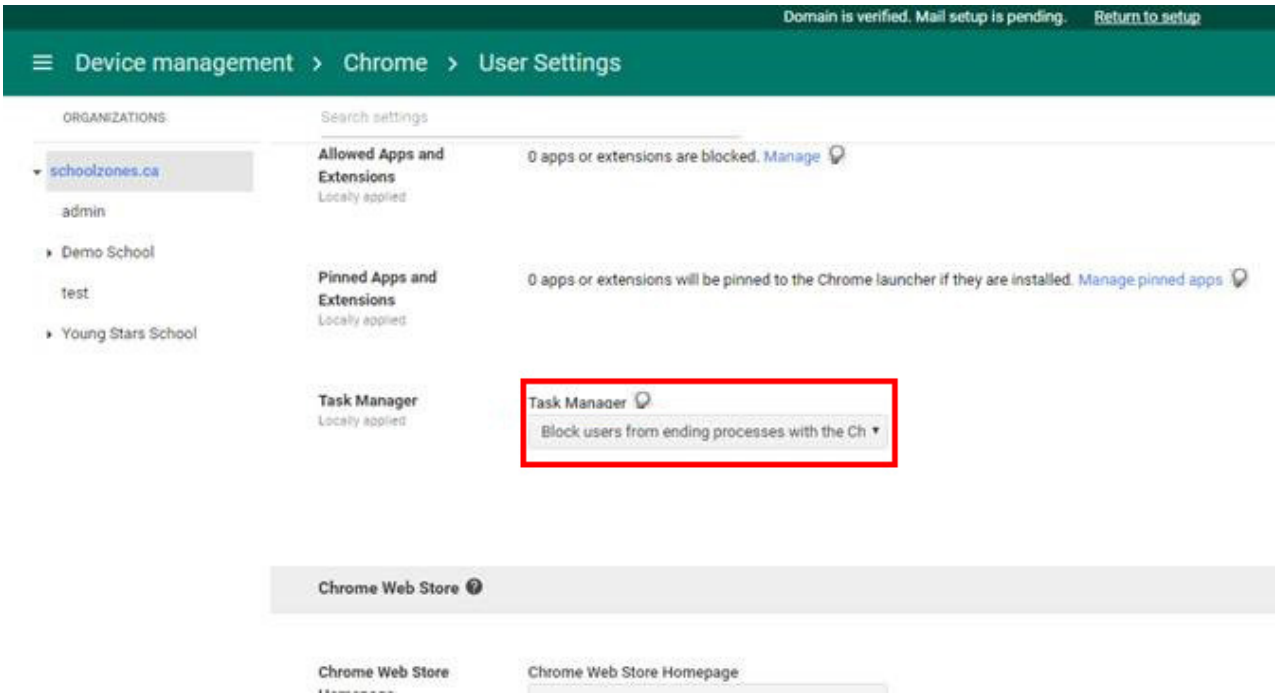
Blocking Task Manager

Task Manager should be blocked for managed Google domains.

To block Task Manager:

1. In the Google Admin console, go to *Device Management* > *Chrome Management* > *User settings* > *Apps and Extensions*.

2. From the left panel, select the organization.
3. Under *Task Manager* select *Block users from ending processes with the Chrome Task Manager* from the dropdown list.



4. Click *Save*.

Service Account Credentials

FortiClient EMS for Chromebooks requires service account credentials generated by the Google Developer console. You can use the default service account credentials provided with FortiClient EMS for Chromebooks or generate and use unique service account credentials, which is more secure.

The service account credentials must be the same in FortiClient EMS for Chromebooks and the Google Admin console.

This section describes how to configure default and unique service account credentials. See the following sections:

- Configuring default service account credentials on page 21
- Configuring unique service account credentials on page 22

Configuring default service account credentials

FortiClient EMS for Chromebooks includes the following default service account credentials generated by the Google Developer console:

Option	Default Setting	Where Used
Client ID	102515977741391213738	Google Admin console
Email address	account-1@forticlientwebfilter.iam.gserviceaccount.com	FortiClient EMS for Chromebooks
Service account certificate	A certificate in `.pem` format for the service account credentials	FortiClient EMS for Chromebooks

The service account credentials are a set. If you change one credential, you must change the other two credentials.

Adding the default service account client ID to the Google Admin console

To configure the default service account credentials, you must add the client ID's default value to the Google Admin console. No other configuration for service account credentials is required. See Adding service account credentials to the Google Admin console on page 25.

Configuring unique service account credentials

When using unique service account credentials for improved security, you must complete the following steps to add the unique service account credentials to the Google Admin console and FortiClient EMS for Chromebooks:

1. Create unique service account credentials using the Google Developer console. See Creating unique service account credentials on page 22.
2. Add the unique service account credentials to the Google Admin console. See Adding service account credentials to the Google Admin console on page 25.
3. Add the unique service account credentials to FortiClient EMS for Chromebooks. See Adding service account credentials to EMS on page 26.

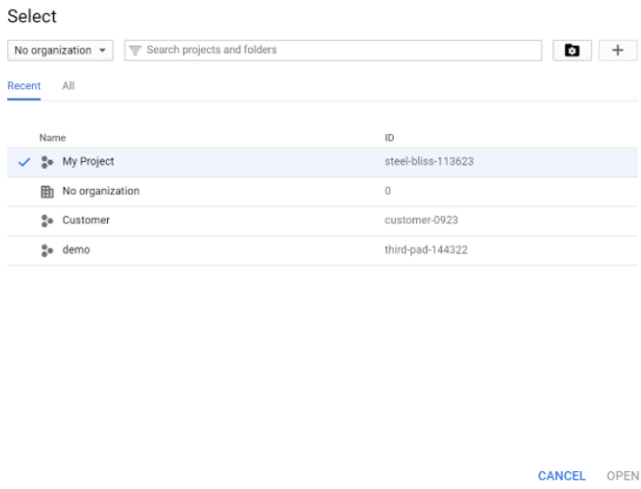
Creating unique service account credentials

Creating a unique set of service account credentials provides more security. Unique service account credentials include the following:

- Client ID (a long number)
- Service account ID (email address)
- Service account certificate (a certificate in `.pem` format)

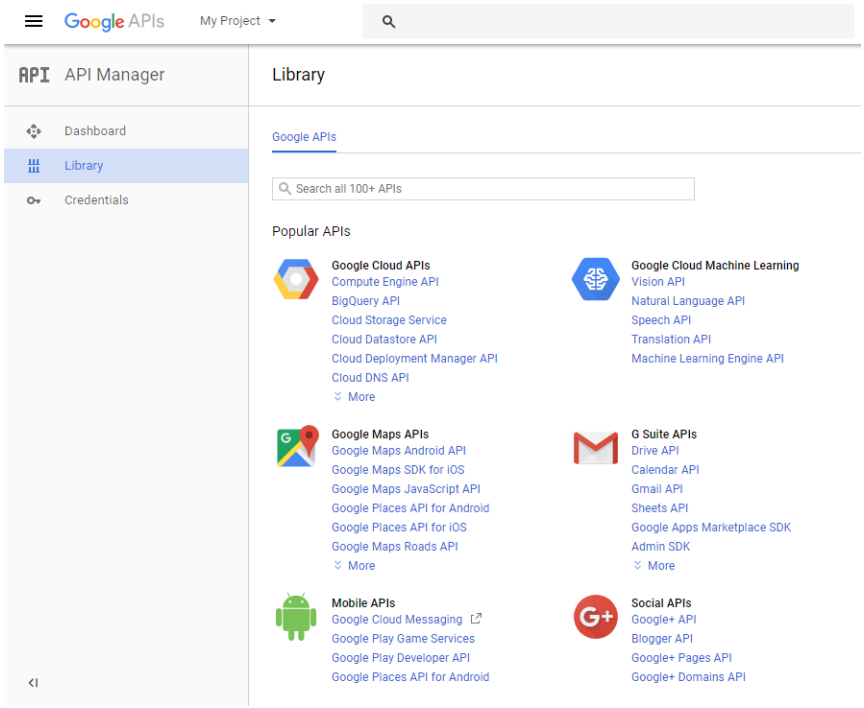
To create a unique service account:

1. Go to https://console.developers.google.com.
2. Log in with your G Suite account credentials.
3. Create a new project:
   a. Click the toolbar list. The browser displays the following dialog.

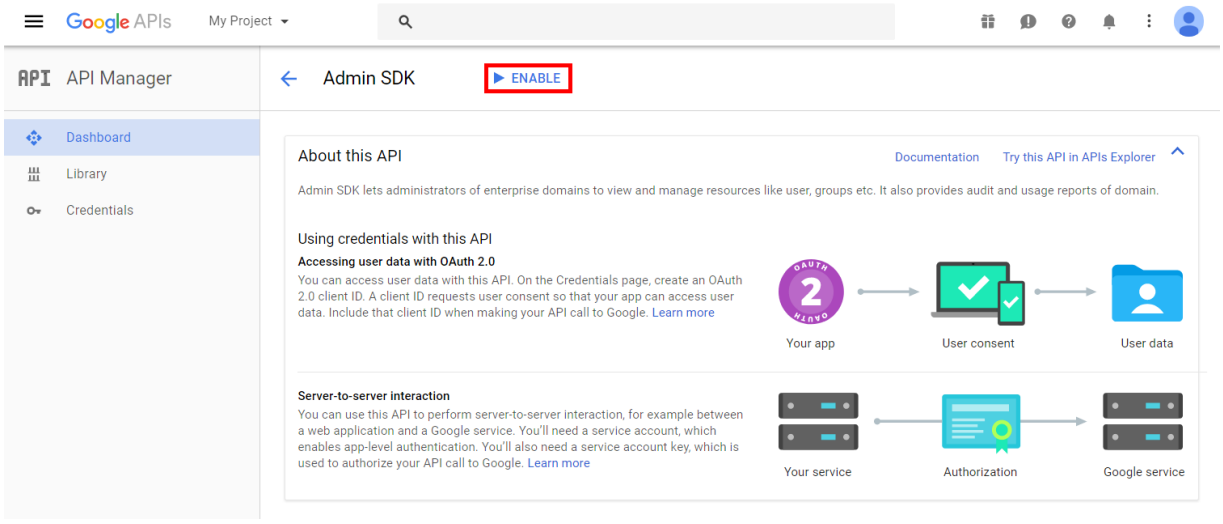


   b. Select your organization, if you see an organization dropdown list.
   c. Click the + button.
   d. In the *Project name* field, enter your project name, then click *Create*.

4. Enable the Admin SDK:
   a. Select your project from the toolbar list, then go to the *Library* tab.
   b. Under *G Suite APIs*, click *Admin SDK*.

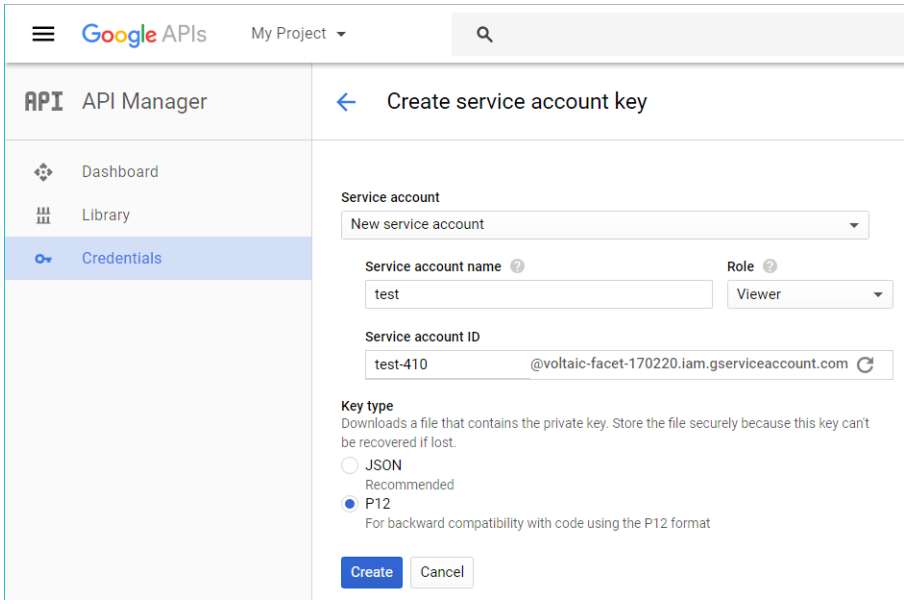


   c. Click *ENABLE*.



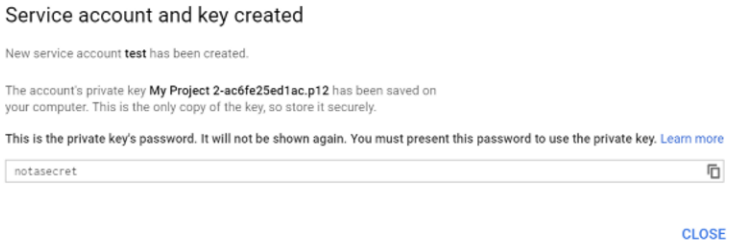
5. Create a service account:
   a. Go to the *Credentials* tab and select *Create Credentials* > *Service account key*.
   b. From the *Service account* list, select *New Service Account*. Enter a service account name.
   c. From the *Role* list, select *Project* > *Viewer*.

d. Select *P12* as the *Key type* and click *Create*.



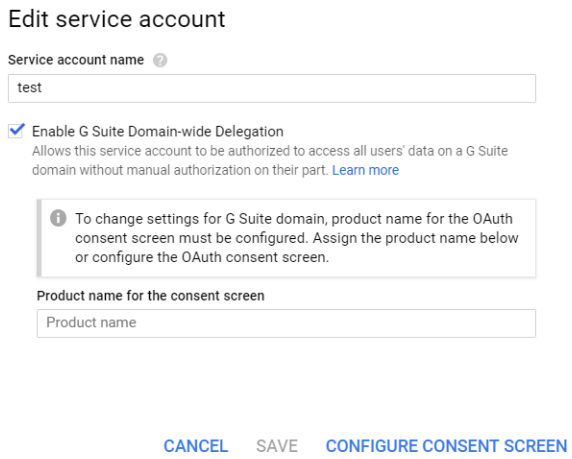
After you create the service account, a private key with the `P12` extension is saved on your computer.

The private key with the `P12` extension is the only copy you will receive. Keep it in a safe place. You should also remember the password prompted on the screen. At this time, that password should be **`notasecret`**.

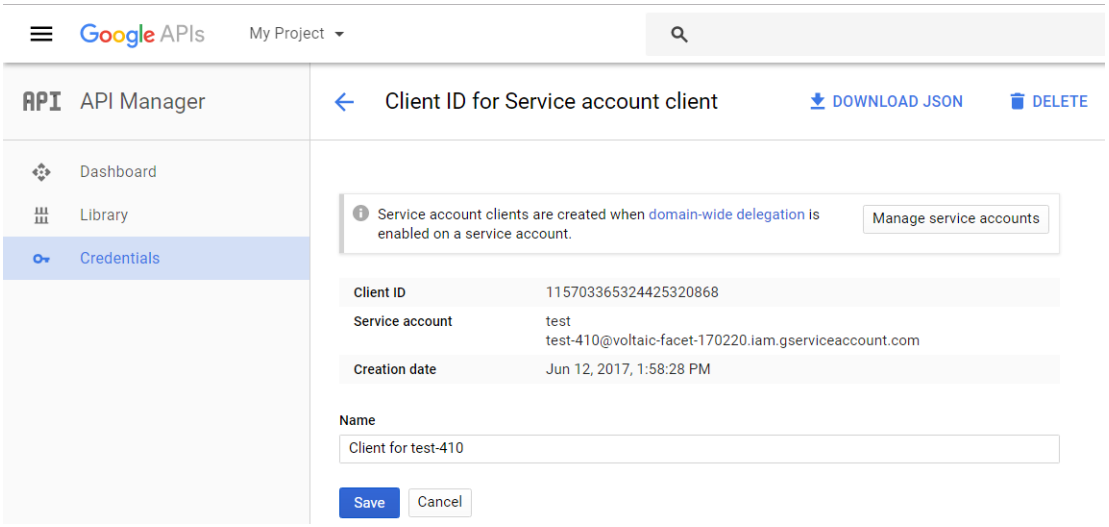


6. Go to the *Credentials* page > *Manage service accounts*.

7. *Edit* the service account you just created and select the *Enable Google Apps Domain-Wide Delegation* checkbox. Enter a *Product name for the consent screen* if this field appears.



8. Click *Save*.
9. Click *View Client ID* to see your service account information. Record the client ID, service account, and the associated private key (downloaded in step 5d).



To use the private key in EMS, it needs to be converted to .pem format. You can use the following openssl command to convert it. Remember to use the notasecret password.

```
C:\OpenSSL-Win64\bin>openssl pkcs12 -in demo-976b9d6e9328.p12 -out
     serviceAccount-demo.pem -nodes -nocerts
Enter Import Password:
```

Adding service account credentials to the Google Admin console

This section describes how to add the client ID from the service account credentials to the Google Admin console. These settings allow Google to trust FortiClient EMS for Chromebooks, which enables FortiClient EMS for Chromebooks to retrieve information from the Google domain.

To add the client ID:

1. In the Google Admin console, go to *Security* > *Advanced settings* > *(you may need to click "show more" to see this)* > *Manage API client access*.
2. Set the following options:
   a. For the *Client Name* option, add the client ID from the service account credentials.
   b. For the *API Scopes* option, add the following string:
   https://www.googleapis.com/auth/admin.directory.orgunit.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly

   The API scopes are case-sensitive and must be lowercase. You may need to copy the string into a text editor and remove spaces created by words wrapping to the second line in the PDF.
3. Click *Authorize*.

Adding service account credentials to EMS

The section describes how to add the service account ID and service account certificate from the service account credentials to FortiClient EMS for Chromebooks.

To add service account credentials:

1. In FortiClient EMS for Chromebooks, go to *System Settings* > *EMS for Chromebook*.

   The default service account credentials display. Overwrite the default settings with the unique set of service account credentials received from Fortinet.
2. The *Service account* field shows the configured email address provided for the service account credentials. Click the *Update service account* button and configure the following information:

ID	Type a new email address for the service account credentials.
Private key	Click *Browse* and select the certificate provided with the service account credentials.

3. Click *Save*.
4. Update the client ID in the Google Admin console.

The service account credentials are a set. If you change one credential, you must change the other two credentials.

FortiClient EMS for Chromebooks Setup

This section describes how to set up FortiClient EMS for Chromebooks. Following is a summary of how to set up FortiClient EMS for Chromebooks:

1. Add an SSL certificate. See Adding SSL certificates on page 27.
2. Add the Google domain. See Adding Google domains on page 29.
3. Create an endpoint profile. See Adding new profiles on page 30.
4. Assign the endpoint profile to the Google domain. See Assigning profiles to Google Chromebooks on page 31.
5. View the status. See Viewing domains on page 32.

Additional configuration procedures are also included in this section.

Adding SSL certificates

This section includes information about the required SSL certificates to support the following types of communication:

- Communication with the FortiClient Chromebook Web Filter extension on page 27
- Communication with FortiAnalyzer for logging on page 28

It includes the following procedures:

- Required: Adding SSL certificates to FortiClient EMS for Chromebooks on page 27
- Required only when sending logs to FortiAnalyzer: Adding SSL certificates to FortiAnalyzer on page 29

Communication with the FortiClient Chromebook Web Filter extension

The FortiClient Chromebook Web Filter extension communicates with FortiClient EMS for Chromebooks using HTTPS connections. The HTTPS connections require an SSL certificate. You must obtain an SSL certificate and add it to FortiClient EMS for Chromebooks to allow the extension to trust FortiClient EMS for Chromebooks.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiClient EMS for Chromebooks. See Adding SSL certificates to FortiClient EMS for Chromebooks on page 27.

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiClient EMS for Chromebooks and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS for Chromebooks will not work. See Uploading root certificates to the Google Admin console on page 17.

Adding SSL certificates to FortiClient EMS for Chromebooks

You must add an SSL certificate to FortiClient EMS for Chromebooks to allow HTTPS connections with the Google Admin console.

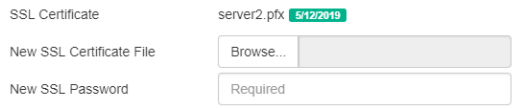
If you are using a public SSL certificate, add the certificate to FortiClient EMS for Chromebooks. You do not need to add the certificate to the Google Admin console.

If you are not using a public SSL certificate, you must add the SSL certificate to FortiClient EMS for Chromebooks, and the root certificate to the Google Admin console. See Adding root certificates on page 15.

To add or replace SSL certificates:

1. In FortiClient EMS for Chromebooks, go to *System Settings* > *EMS for Chromebooks*.
2. Beside *SSL certificate*, click *Update SSL certificate*.
3. Click *Browse* and locate the certificate file (<name>.pfx).
4. In the *Password* box, type the password.
5. Click *Test*.
6. Click *Save*.

If the SSL certificate is expiring in less than three months, the expiry date label is yellow; if it has expired, the label is red. Otherwise, it is green.



Communication with FortiAnalyzer for logging

This section applies only if you are sending logs from FortiClient EMS for Chromebooks to FortiAnalyzer. If you are not sending logs, skip this section.

Sending logs to FortiAnalyzer requires you enable ADOMs in FortiAnalyzer and add FortiClient EMS for Chromebooks to FortiAnalyzer. FortiClient EMS for Chromebooks is added as a device to the FortiClient ADOM in FortiAnalyzer. See the *FortiAnalyzer Administration Guide*.

FortiClient EMS for Chromebooks supports logging to FortiAnalyzer. If you have a FortiAnalyzer device and configure FortiClient EMS for Chromebooks to send logs to FortiAnalyzer, a FortiAnalyzer CLI command must be enabled and an SSL certificate is required to support communication between the FortiClient Web Filter extension and FortiAnalyzer.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiAnalyzer. See Adding SSL certificates to FortiAnalyzer.

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiAnalyzer and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiAnalyzer will not work. See Uploading root certificates to the Google Admin console on page 17.

The FortiAnalyzer IP address should be specified in the SSL certificate. If you are using a public SSL certificate, the FortiAnalyzer IP address can be assigned to *Common Name* or *Alternative Name*. If you are using a self-signed (nonpublic) SSL certificate, your certificate's *Subject Alternative Name* must include `IP:<FortiAnalyzer IP>`.

Enabling HTTP and HTTPS logging access to FortiAnalyzer

You must use the FortiAnalyzer CLI to add HTTP-logging and HTTPS-logging to the allow-access list in FortiAnalyzer. This command is one step in the process that allows FortiAnalyzer to receive logs from FortiClient EMS for Chromebooks.

In FortiAnalyzer CLI, enter the following command:

```
config system interface
   edit "port1"
      set allowaccess https ssh http http-logging https-logging
   next
end
```

Adding SSL certificates to FortiAnalyzer

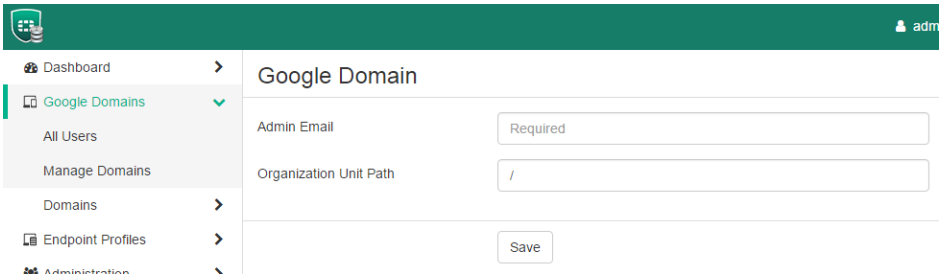
To add SSL certificates to FortiAnalyzer:

1. In FortiAnalyzer, go to *System Settings* > *Certificates* > *Local Certificates*.
2. Click *Import*. The *Import Local Certificate* dialog appears.
3. In the *Type* list, select *Certificate* or *PKCS #12 Certificate*.
4. Beside *Certificate File*, click *Browse* to select the certificate.
5. Enter the password and certificate name.
6. Click *OK*.

Adding Google domains

To add Google domains:

1. Go to *Google Domains* > *Manage Domains*, and click the *Add* button. The *Google Domain* pane displays.



2. In the *Admin Email* box, type your Google domain admin email.
3. In the *Organization Unit Path* box, type the domain organization unit path.

/ stands for the root of the domain.

4. Click *Save*.
   The Google domain information and users are imported into FortiClient EMS for Chromebooks.

Configuring profiles

Profiles support web filtering by categories, black and white lists, and safe search. You can create different profiles and assign them to different groups in the Google domain.

Adding new profiles

When you install FortiClient EMS for Chromebooks, a default profile is created. This profile is applied to any domains you add to FortiClient EMS for Chromebooks.

It is recommended to add Yandex search engine to the black list in the profile.

To create new profiles:

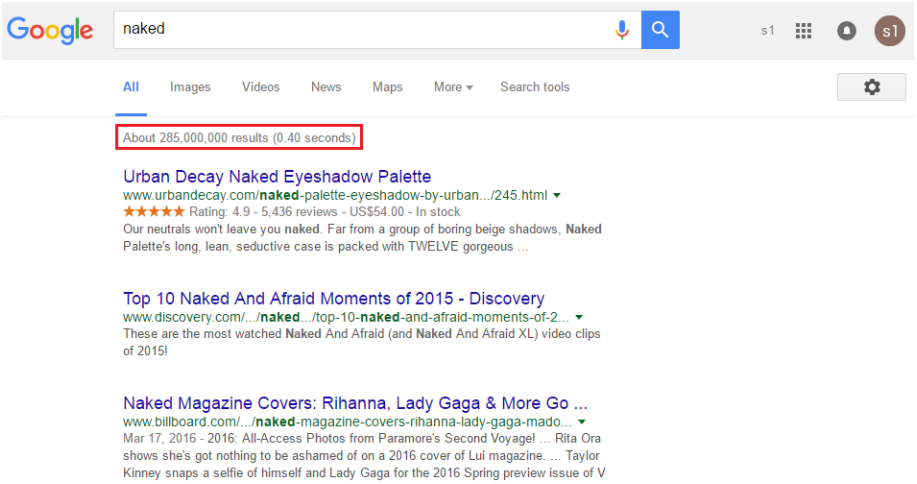
1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add* button.
2. In the *Profile Name* box, type the profile name.
3. On the *Web Filter* tab, enable *Web Filter*, and set the web filtering options.
4. On the *System Settings* tab, set the logging options.
5. Click *Save*.

Enabling/disabling Safe Search

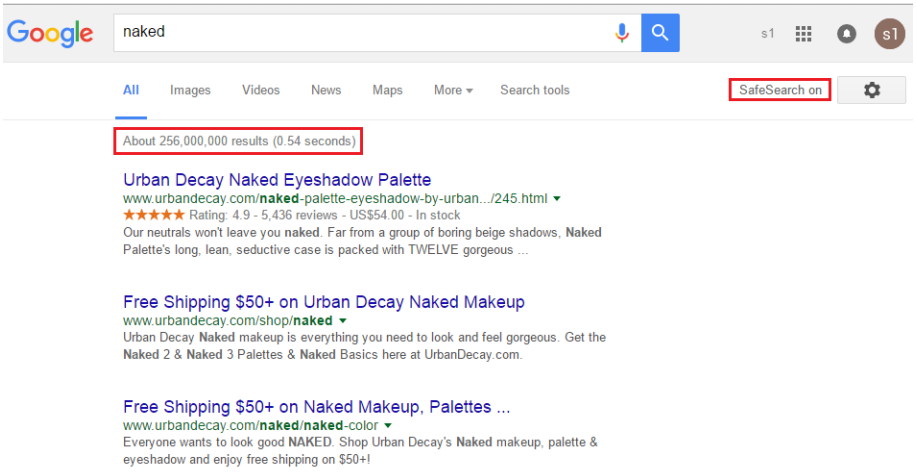
The search engine provides a Safe Search feature that blocks inappropriate or explicit images from search results. The Safe Search feature helps avoid most adult content. FortiClient EMS for Chromebooks supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

The profile in FortiClient EMS for Chromebooks controls the Safe Search feature.

Following are examples of search results with the Safe Search feature disabled and enabled. Notice the difference between the number of results. Here are the search results when the Safe Search feature is disabled, which has about 285000000 results:



Here are the search results when the Safe Search feature is enabled, which has about 256000000 results.



To enable or disable Safe Search:

1. In FortiClient EMS for Chromebooks, in the *Endpoint Profiles* area, click the *Default* profile or another profile.
2. On the *Web Filter* tab, enable or disable *Enable Safe Search*.

Assigning profiles to Google Chromebooks

After creating the profile, you can assign the profile to Google domains. When you assign the profile to domains, the profile settings are automatically pushed to the Chromebooks in the domain.

To assign profiles:

1. Go to *Google Domains*.
2. Right-click a domain, select *Assign Profile*, then the profile. The profile is assigned.
3. Hover the mouse over the name of the domain to view the name of the assigned profile.

Viewing domains

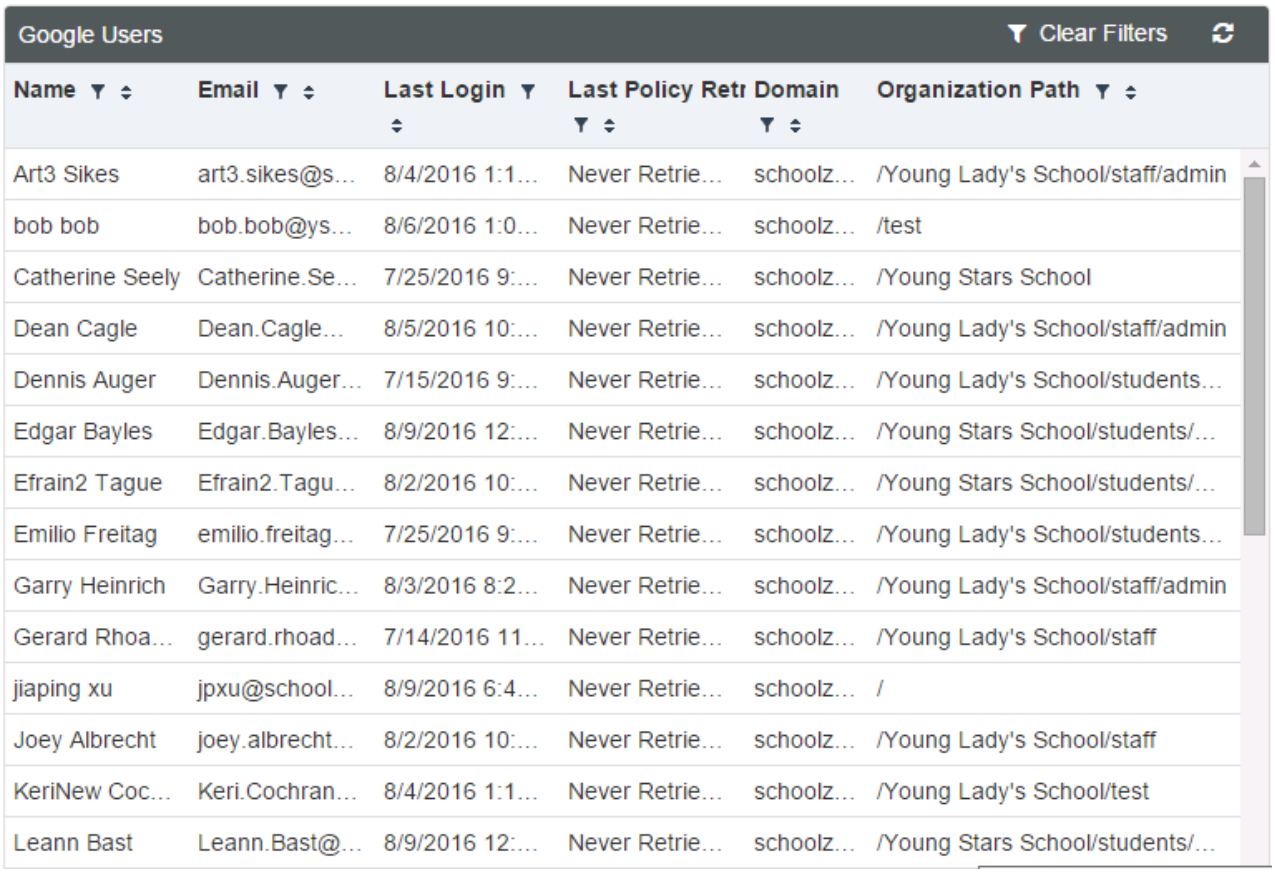
After you add domains to FortiClient EMS for Chromebooks, you can view the list of domains in *Google Domains*. You can also view the list of Google users in each domain and details about each Google user in the *User Details*, *Client Statistics*, and *Blocked Sites* panes.

Viewing the Google Users pane

You can view Google users' information in FortiClient EMS for Chromebooks.

To view the Google Users pane:

1. Go to *Google Domains* > *Domains* and click a domain. The list of Google users displays.



The following options are available in the toolbar:

Clear Filter (filter icon)	Click the Clear Current Filter icon to clear the currently used filter.
Refresh	Click the Refresh icon to refresh the page.

The following columns of information are displayed for Google users:

Name	Chromebook user's name.

Email	Chromebook user's email address.
Last Login	Date and time when the user last logged into the domain.
Last Policy Retrieval	Date and time of the last endpoint profile retrieved by the Google Chromebook.
Domain	Name of the domain to which the user belongs.
Organizational Path	Organization path in the domain.

Viewing user details

You can view details about each user in a Google domain.

To view user details:

1. Go to *Google Domains* > *Domains*. The list of domains displays.
2. Click a domain. The list of Google users displays.
3. Click a Google user and scroll to the bottom of the content pane. The *User Details*, *Client Statistics*, and *Blocked Sites* panes display.

User Details

Field	Information
Name	User's name.
Email	User's email address.
Last Login	Date and time when the user last logged into the domain.
Last Policy Retrieval	Date and time of the last endpoint profile retrieved by the Google Chromebook.
Organization Path	Organization path of the user in the domain.
Effective Policy	Name of the profile assigned to the user in the domain.

Client Statistics

Charts	Information
Blocked Sites Distribution (past <number> days)	Displays the distribution of blocked sites in the past number of days. You can configure the number of days for which to display information. Go to *System Settings* > *Logs*.
Top 10 Site Categories by Distribution (Past <number> Days)	Displays the distribution of top ten site categories in the past number of days. You can configure the number of days for which to display information. Go to *System Settings* > *Logs*.

Blocked Sites (Past <number> Days)

Fields	Information
Time	Time the blocked site was visited.
Threat	Threat type detected.
Client Version	Chromebook user's current version.
OS	Type of OS used by the Chromebook user.
URL	Blocked site's URL.
Port	Port number currently listening.
User Initiated	User initiated visitation to the blocked site.

Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.